UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,110	08/10/2006	Begonya Otal	DE040036US1	6042

24738 7590 12/21/2007
PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
INTELLECTUAL PROPERTY & STANDARDS
370 W. TRIMBLE ROAD MS 91/MG
SAN JOSE, CA 95131

EXAMINER	
TABOR, AMARE F	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
12/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	**Application No.** 10/589,110	**Applicant(s)** OTAL ET AL.	
	Examiner Amare Tabor	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *10 August 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *08/10/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-15 are examined.

Specification

2. The disclosure is objected to because of the following informalities:

a. Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

b. In the Specification

On page 13 and the 3rd paragraph in page 14, the encryption module shown in Fig. 2a is referred as "***26***"; however, the reference number for the encryption module in Fig. 2a is "***28***". Additionally, in the 4th and 5th paragraphs of page 15, the encrypted data is referenced as "***42***"; however, the corresponding reference number in Fig. 4 is "***4***".

Appropriate Correction is required.

Claim Objections

3. Claims 1 and 3 are objected to because of the following informalities: in the last limitation of claims 1 and 3, the word "***were***" is read as "***where***" for examining. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 9 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 9 recites the limitation, "*where (k m) each receiver set of keys contains a number m of said keys base; and where is substantially greater than N.*" The language of this limitation is not clear. In claim 15, the claim language "*method for operating a system including ...*" is not clear. The claim should either be a method or a system claim; but not both. Therefore, claims 9 and 15 are rejected as being indefinite and/or unclear.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni et al. (US 6,049,878 referred as "***Caronni***" hereinafter) in view of "***Hardjono***" (US 6,584,566 B1).

As per Claim 1, Caronni teaches,

System for selective data transmission (see *abstract*) with a sender (see *100 & 300* in *fig. 1 &* 3) and at least a first and a second receiver (see *101 & 301* in *fig. 1 &* 3);

- with encryption means (see *TRAFFIC ENCRYPTION 106* in *Fig .*1) associated with said sender said encryption means comprising a plurality of base keys (see *GROUP KEY MANAGEMENT 108* in *Fig. 1*);

- a transmission channel (see *NET* in *Fig .1* or *302* in *Fig.* 3) from said sender to said receivers for transmission of encrypted data (see *Fig. 2 for encrypted data*);

- and with decryption means (see *TRAFFIC DECRYPTION 107* in *Fig .*1) associated with each of said receivers said decryption means each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys (see *PARTICIPANT KEY MANAGEMENT 109* in *Fig. 1*);

- where for transmission of data at least to said second receiver (see *X0-X7* in *Fig. 5*), said encryption means are configured to encrypt said data recursively (see *Fig. 6 for recursive* encryption) with at least two keys said keys being comprised in said receiver set of said second receiver (see *Fig. 6; the system of Caronni uses one key in re-keying*), and at least one of said keys not being comprised in said receiver set of said first receiver (see *Fig.* 4; and for example, column 8, line 33 to column 9, line 9);

- and where said decryption means of said second receiver are configured to decrypt said data recursively with said at least two keys (see *Fig. 4-6; the TRAFFIC DECRYPTION 107 of the RECEIVER 101* in *Fig. 1 decrypts recursively by reversing for encryption process done by the TRAFFIC ENCRYPTION 106 of the SENDER 100* in *Fig. 1*).

Caronni fails to teach explicitly comprising at least two keys. However, in the same field of endeavor, Hardjono teaches comprising at least two keys (see *Fig. 2 & 4*; and for example, column 4, lines 53-62).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to combine the teachings of Hardjono and Caronni because both inventions are directed to multicasting communication systems. One having ordinary skill in the art would be motivated to modify the teaching of Caronni by adding at least two keys as taught by Hardjono in order to decrease the scalability problems associated with member joining/ leaving group (see column 2, lines1 to column 3, line 4 of Hardjono).

As per Claim 2, Caronni teaches,

System according to claim 1, said system further comprising a third receiver (see *X0-X7* in *Fig. 5*) with decryption means (see *TRAFFIC DECRYPTION 107* in *Fig* .1) comprising a receiver set of keys which is a subset of said base keys (see *PARTICIPANT KEY MANAGEMENT 109* in *Fig. 1*);

- where said receiver sets of said first, second and third receiver are pair-wise different (see *X0-X7* in *Fig. 5; the receivers are grouped to be pair-wise different*);

- and where said receiver set of said second receiver and said receiver set of said third receiver comprise at least two common keys where at least one of said at least two common keys is not comprised in said receiver set of said first receiver (see *Fig. 5; second, third, ... set of receivers are disclosed; however, the groups have only one common key*);

- and where for transmission of data to a group at least comprising said second receiver said third receiver said encryption means are configured to encrypt said data recursively with at least said two common keys (see *Fig. 6 for recursive* encryption);

- and where said decryption means of said second and third receiver are each configured to decrypt said data recursively with at least said two common keys (see *Fig. 4-6; the TRAFFIC DECRYPTION 107 of the RECEIVER 101* in *Fig. 1 decrypts recursively by reversing for encryption process done by the TRAFFIC ENCRYPTION 106 of the SENDER 100* in *Fig. 1*).

Caronni fails to teach explicitly using at least two common keys. However, Hardjono teaches using at least two common keys (see *Fig.*2 & *4*; and for example, column 4, lines 53-62).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to modify the teaching of Caronni by adding at least two keys as taught by Hardjono in order to decrease the overhead caused when a recipient leaves the system.

As per Claim 3, Caronni teaches,

System for selective data transmission according to claim 1 with a plurality of receivers each with associated decryption means (see *TRAFFIC DECRYPTION 107* in *Fig* .1) with a receiver set of keys (see *PARTICIPANT KEY MANAGEMENT 109* in *Fig. 1*), where said receiver sets are pair-wise different (see *X0+X1, X2+X3, ..., X6+X7* in *Fig. 5; the receivers are grouped to be pair-wise different*);

- where an authorized group of said receivers is authorized to receive said data (see *Fig. 5; for authorized group of receivers*);

- and where for transmission of said data to the receivers of said authorized group, said encryption means (see *TRAFFIC ENCRYPTION 106* in *Fig* .1) are configured to encrypt said data recursively with a plurality of keys all of said keys being comprised in said receiver sets of the receivers of said authorized group (see *Fig. 6 for recursive* encryption), and for each receiver not belonging to said authorized group at least one of said keys not being comprised in the corresponding receiver set (see *Fig. 6; the system of Caronni uses one key in re-keying and for additional keys see rejection of claims 1 and 2 above*);

- and where said decryption means of the receivers of said authorized group are configured to decrypt said data recursively with said plurality of keys (see *Fig. 4-6; the TRAFFIC DECRYPTION 107 of the RECEIVER 101* in *Fig. 1 decrypts recursively by reversing for encryption process done by the TRAFFIC ENCRYPTION 106 of the SENDER 100* in *Fig. 1*).

As per Claim 4, Caronni teaches,

System according to claim 3, where said authorized group of receivers is divided into at least two subgroup (see *Fig. 5; KEK K03 & K47 are shared among four participants)*;

- and for transmission of said data to the receivers of said authorized group, said data is transmitted to said receivers in at least two transmissions (see *Fig. 5;*), where in each transmission the data is encrypted recursively with a different set of keys (see *Fig. 6 for recursive* encryption), all of said keys being comprised in said receiver sets of the corresponding subgroup of receivers (see *rejections of claims 1 & 2*).

As per Claim 5, Caronni teaches,

System according to claim 1, where said encryption means (see *TRAFFIC ENCRYPTION 106* in *Fig* .1) are configured for recursive encryption with a plurality of encryption steps, where in each encryption step a piece of data is encrypted with a key to calculate an encrypted piece of data (see *Fig. 6 for recursive* encryption) ;

- where each of said encryption steps includes calculation of at least one exponentiation with a key number associated with said key (see *Fig. 6*);

- and said encryption means being configured to recursively apply said encryption steps with a plurality of keys by multiplying key numbers associated with said keys, and calculating an exponentiation with the result of said multiplication (see *Fig. 6; multiplying keys and exponentiation calculation is well known in the art, for example in RSA, Diffie/Hellman etc*; and for example, column 2, lines 50-67).

As per Claim 6, Caronni teaches,

System according to claim 1, with a plurality of receivers, where said receivers are divided into a plurality of groups (see *Fig. 5; KEK K03 & K47 are shared among four participants)*;

- where for each of said groups the encryption means comprise a group set of base keys (see *GROUP KEY MANAGEMENT 108* in *Fig. 1*), said group sets being pair-wise different from each other (see *X0+X1, X2+X3, ..., X6+X7* in *Fig. 5; the receivers are grouped to be pair-wise different*);

- and the decryption means (see *TRAFFIC DECRYPTION 107* in *Fig* .1) of each of said receivers comprise a receiver set of keys (see *set of keys* in *Fig. 5*), which is a subset of the group set of the group that the respective receiver is a member of (see *Fig. 5*) .

As per Claim 7, Caronni teaches,

System according to claim 1, with a plurality of receivers (see *X0-X7* in *Fig.* 5) with decryption means (see *TRAFFIC DECRYPTION 107* in *Fig* .1) associated with each of said receivers said decryption means each comprising a receiver set of keys (see *keys K01, K03,...* in *Fig. 5*), where each receiver set of keys is a subset of said base keys (see *GROUP KEY MANAGEMENT 108* in *Fig. 1*; and *TEK* in *Fig. 4*);

- where each of said receiver sets of keys comprises the same number of base keys (see *Fig. 5*).

As per Claim 8, Caronni teaches,

System according to claim 1 with a plurality of receivers, and storage means (see *Fig. 4; abstract;* and for example, column 10, lines 13-35) associated with said sender which store information about a first, authorized group of receivers out of said plurality of receivers, and/or about a second, unauthorized group of receivers out of said plurality of receivers (*the GROUP and PARTICIPANT KEY MANAGEMENT* in *Fig. 1* and *3 have data structure to store and manage keys*);

- where said sender comprises distribution control means (see *ADMISSION CONTROL 110* in *Fig. 1*) for controlling message transmission, said distribution control means being configured to determine one or more combinations of said base keys such that messages recursively encrypted with said combinations are decryptable only at said receivers belonging to a first group, and are not decryptable at said receivers belonging to said second group (see *Fig. 1 & 3;* and for example, column 4, line 7 to column column 7, line 67).

As per Claim 9, Caronni teaches,

System according to claim 1, with a number k of base keys; and a number N of receivers, and with decryption means associated with each of said receivers, said decryption means each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys; where each receiver set of keys contains a number m of said keys base (see column 5, line 59 to column 9, line 65)

Caronni fails to teach explicitly where (k m) is substantially greater than N. However, Caronni teaches (2*N)-1 greater that N (see column 5, line 66 to column 6, line 39; *it is obvious that (2*N)-1) is substantially greater than N*).

It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Caronni by including (k m). One skilled in the art would be motivated to substitute one method for the other because (2*N)-1 is substantially greater than N and the modification increases sender's efficiency of key distribution.

As per Claim 10, Caronni teaches,

Sender (see *100 & 300* in *fig. 1* & 3) for use in a transmission system according to claim 1, with encryption means comprising a plurality of base keys said encryption means being configured to encrypt data recursively with at least two of said base keys (see *TRAFFIC ENCRYPTION 106, GROUP KEY MANAGEMENT 108* in *Fig. 1* and *Fig. 6*);

- and transmission means for transmitting said encrypted data over a transmission channel (see *NET* in *Fig .1* or *302* in *Fig.* 3).

As per Claim 11, Caronni teaches,

Receiver (see *101 & 301* in *fig. 1* & 3) for use in a transmission system according to claim 1, with receiving means for receiving encrypted data of a transmission channel (see *Fig. 1 & 3*);

- and decryption means comprising a receiver set of keys (see *TRAFFIC DECRYPTION 107 and PARTICIPANT KEY MANAGEMENT 109* in *Fig. 1*); where said decryption means are configured to decrypt said encrypted data recursively with at least two of said keys (see *Fig. 4-6; the TRAFFIC DECRYPTION 107 of the RECEIVER 101* in *Fig. 1 decrypts recursively by reversing for encryption process done by the TRAFFIC ENCRYPTION 106 of the SENDER 100* in *Fig. 1*).

As per Claim 12, Caronni teaches,

Broadcasting system with scrambling means for scrambling content with a scrambling key (see *Fig. 1 & 3; abstract*; and for example, column 4, lines 7-50);

- a broadcasting sender for broadcasting said scrambled content over a channel (see *SENDER MULTICAST APPLICATION* in *Fig. 1 & 3*);

- said broadcasting system further comprising a selective data transmission system according to claim 1 with a sender and receivers for selectively transmitting the scrambling key (see *Fig. 1* & 3);

- where said receivers each comprise de-scrambling means for de-scrambling said scrambled content with said scrambling key (see *TRAFFIC DECRYPTION* and *PARTICIPANT KEY MANAGEMENT* in *Fig. 1 & 3*).

As per Claim 13, Caronni teaches,

Method for selective data transmission, where encrypted data is transmitted from a sender comprising a plurality of base keys (see *Fig. 1 & 3; abstract*);

- to at least a first and a second receiver (see *101 & 301* in *fig. 1* & 3) each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys (see *PARTICIPANT KEY MANAGEMENT* in *Fig. 1 & 3*);

- where for selective transmission of data two set second receiver (see *X0-X7* in *Fig. 5*) said method includes the following steps: at said sender encrypting said data recursively (see *Fig. 6 for recursive* encryption) with at least two keys said keys being comprised in said receiver set of said second receiver (see *Fig. 6; the system of Caronni uses one key in re-keying*), and at least one of said keys not being comprised in said receiver set of said first receiver and transmitting the encrypted data over a transmission channel (see *Fig.* 4; and for example, column 8, line 33 to column 9, line 9);

- and, at said second receiver decrypting said encrypted data recursively with said at least two keys (see *Fig. 4-6; the TRAFFIC DECRYPTION 107 of the RECEIVER 101* in *Fig. 1 decrypts recursively by reversing for encryption process done by the TRAFFIC ENCRYPTION 106 of the SENDER 100* in *Fig. 1*).

Caronni fails to teach explicitly encrypting and decrypting using at least two common keys. However, Hardjono teaches encrypting and decrypting using at least two common keys (see.

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's invention to modify the teaching of Caronni by adding at least two keys as taught by Hardjono in order to decrease the overhead caused when a recipient leaves the system.

As per Claim 14, Caronni teaches,

Method according to claim 13, said method further comprising the steps of determining at least one base key to exchange (see *GROUP* and *PARTICIPANT KEY MANAGEMENT* in *Fig. 1*);

- generating at least one new base key (*GROUP KEY MANAGEMENT generates new base keys*);

- and encrypting the new base key recursively with a plurality of base keys (see *Fig. 6*), and transmitting the thus encrypted key to a plurality of receivers (see *Fig. 5*).

As per Claim 15, Caronni teaches,

Method (see *abstract*) for operating a system including a sender (see *100 & 300* in *fig. 1* & 3) and a plurality of receivers (see *101 & 301* in *fig. 1* & 3; and *x0-X7* in *Fig. 5 for plurality of receivers*) said method comprising the steps of:

- determining an issuing scheme (*Caronni discloses five stages or states in* operation) for issuing a number of base keys to a number of receivers where each of said receivers holds a number of said base keys (see column 5, line 59 to column 6, line 65);

- generating said base keys (*GROUP KEY MANAGEMENT generates new base keys*);

- and, upon joining of said receivers distributing said base key to said receivers according to said predetermined issuing scheme (see column 7, lines 7-67).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
AU 2139

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100